IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR KING COUNTY

SHAWNA ARNESON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FRED HUTCHINSON CANCER CENTER, a Washington Nonprofit Corporation,

Defendant.

NO.

CLASS ACTION COMPLAINT

CLASS ACTION COMPLAINT

Plaintiff Shawna Arneson ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Defendant Fred Hutchinson Cancer Center ("Defendant" or "Fred Hutch"). Plaintiff brings this action by and through her attorneys, and alleges, based upon personal knowledge as to her own actions, and based upon her information and belief and reasonable investigation by her counsel as to all other matters, as follows.

I. INTRODUCTION

1. Fred Hutch is a is a cancer research institute based in Seattle, Washington, and is a preeminent leader in cancer care as well as cancer and infectious disease research. Fred Hutch operates eleven clinical care sites in Washington that provide medical oncology, infusion, radiation, proton therapy and related services to cancer patients. Fred Hutch treats thousands of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

patients each year; in 2022, Fred Hutch provided care to over 50,000 individuals diagnosed with and at risk for cancer.[1]

2. As part of its operations, Fred Hutch collects, maintains, and stores highly sensitive personal and medical information belonging to its patients, including, but not limited to: first and last names, addresses, Social Security numbers, dates of birth (collectively, "personally identifying information" or "PII"), health insurance information, information concerning patients' medical history, mental or physical conditions, and medical diagnosis and treatment (collectively, "private health information" or "PHI") (PII and PHI collectively are "Private Information").

3. On or about November 19, 2023, Fred Hutch detected an incident in which unauthorized cybercriminals accessed information on its clinical network (the "Data Breach"). Upon information and belief, the cybercriminals accessed and stole Private Information belonging to the Plaintiff and Class members. Fred Hutch asserts that when it discovered the unauthorized access, it "immediately notified federal law enforcement and engaged a leading forensic security firm to investigate and contain the incident," and it also took its "clinical network offline and implemented additional information technology security protocols."[2]

4. Since the incident hundreds of Fred Hutch patients have received threatening emails from cybercriminals. In these emails, cybercriminals claim that information for 800,000 patients was stolen in the Data Breach—including names, social security numbers, medical and

[1] *About Fred Hutch: 2022 Annual Report, Fred Hutch Cancer Center*, https://www.fredhutch.org/en/about/about-the-hutch/annual-report.html (last visited Dec. 7, 2023).

[2] *Update on Data Security Incident*, Fred Hutch Cancer Center, https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

insurance information, lab results and more—and demands payment to prevent the sale of that data.[3]

5. On or about December 6, 2023, Fred Hutch sent an email to all current and former patients notifying them of the Data Breach, and instructing all patients to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closed."[4]

6. As Fred Hutch stored and handled such highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

7. Ultimately, Fred Hutch failed to fulfill these obligations as unauthorized cybercriminals breached Fred Hutch's information systems and databases, and upon information and belief, stole vast quantities of Private Information belonging Plaintiff and Class members. This breach—and the successful compromise of Private Information—were direct, proximate, and foreseeable results of multiple failings on the part of Fred Hutch.

8. The Data Breach occurred because Fred Hutch inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. Fred Hutch also inexcusably failed to timely detect this Data Breach. And before the breach occurred, Fred Hutch failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and the Class members been made aware of this fact, they would have never provided such information to Fred Hutch.

---

[3] Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*, KUOW (Dec. 6, 2023), https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack (last visited Dec. 7, 2023).

[4] This Email Notice, which contains information regarding the data security breach incident, is attached as **Exhibit A**.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

9. As a result of Fred Hutch's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Fred Hutch's possession and is subject to further unauthorized disclosures so long as Fred Hutch fails to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Fred Hutch's failure to reasonably safeguard Plaintiff's and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiff's and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, and protection of their Private Information.

II. PARTIES

11. Plaintiff Shawna Arneson is a resident and citizen of the State of Washington and a current patient of Fred Hutch. On December 6, 2023, Plaintiff Arneson received an email from Fred Hutch notifying her of the Data Breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

12. Defendant Fred Hutchinson Cancer Center is a Washington nonprofit corporation with its principal place of business located at 1100 Fairview Ave. N., Seattle, WA 98109-1024. Fred Hutch conducts business in this County and throughout Washington State. Fred Hutch provides medical services and treatments to patients at its 11 clinical sites located across the Puget Sound region. Its main campus—and the home if its cancer research center—is in the South Lake Union area of Seattle, Washington.

III. JURISDICTION AND VENUE

13. This Court has jurisdiction under the Washington Constitution, Article IV, Section 6, and RCW 2.08.010. This Court has jurisdiction over Fred Hutch because Fred Hutch is a resident and citizen of the State of Washington, and its headquarters is in King County.

14. Venue is proper in this County under RCW 4.12.025 because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this County and because Defendant resides in this County.

IV. FACTUAL ALLEGATIONS

A. Fred Hutch – Background

15. In April 2022, Fred Hutchinson Cancer Center was created by way of a merger of Fred Hutchinson Cancer Research Center merged with the Seattle Cancer Care Alliance (SCCA). The result of unifying these research and patient care entities was the creation of a unified adult cancer research and care center that is clinically integrated with University of Washington (UW) Medicine and UW Medicine's cancer program. The purpose of this merger was to integrate scientific endeavors and clinical care to ensure patients have access to the most

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

innovative care. As a result of the restricting, Fred Hutch now serves as UW Medicine's cancer program.[5]

16. Fred Hutch is an independent organization that specializes in cancer care as well as cancer and infectious disease research. Fred Hutch operates through its campus headquarters in Seattle and its eleven clinical care sites across the Puget Sound region of Washington, which provide medical oncology, infusion, radiation, proton therapy and related services to cancer patients.

17. In order to provide healthcare and related research services, Fred Hutch collects, maintains, and stores the highly sensitive PII and PHI provided by its current and former patients, including but not limited to: first and last name, Social Security number, date of birth, health insurance policy number, and information about medical history, mental or physical condition, or medical diagnosis or treatment.

18. As a result of Fred Hutch's relationship with UW Medicine, its computer systems and networks also house some University of Washington Medicine patient data.[6]

19. On information and belief, Fred Hutch failed to implement necessary data security to protect Plaintiff's and Class members' Private Information at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of Fred Hutch's current and former patients—Plaintiff and Class members.

20. Current and former patients of Fred Hutch, such as Plaintiff and Class members, made their Private Information available to Fred Hutch with the reasonable expectation that any

---

[5] *Hutch News Stories: Fred Hutch and Seattle Cancer Care Alliance unite, reshape relationship with UW Medicine*, Fred Hutch Cancer Center (Apr. 1, 2022), https://www.fredhutch.org/en/news/center-news/2022/04/fred-hutch-scca-restructure.html (last visited Dec. 7, 2023).

[6] Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*, KUOW (Dec. 6, 2023), https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack (last visited Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. And, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

21. This expectation was objectively reasonable and based on an obligation imposed on Fred Hutch by statute, regulations, industry standard, and standards of general due care.

22. Unfortunately for Plaintiff and Class members, Fred Hutch failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

23. On November 19, 2023, Fred Hutch detected that cybercriminals had engaged in unauthorized activity on its clinical network. Upon detecting the incident, Fred Hutch engaged a specialized third-party forensic security firm to assist with containing its network and investigating the extent of unauthorized activity.[7] The cybersecurity incident specifically involved Fred Hutch's clinical systems, but those systems also house University of Washington Medicine patient data.[8]

24. Upon information and belief, cybercriminals successfully breached Fred Hutch's systems in the Data Breach and accessed Private Information of current and former Fred Hutch

[7] *Update on Data Security Incident*, Fred Hutch Cancer Center, https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited Dec. 7, 2023).

[8] Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*, KUOW (Dec. 6, 2023), https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack (last visited Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

patients, including their first and last name, date of birth, Social Security number, medical information, diagnosis and treatment information, and health insurance information.[9]

25. Immediately following the Data Breach, hundreds of Fred Hutch patients have received threatening emails from cybercriminals related to the Data Breach. "The emails claim that information for 800,000 Fred Hutch patients was compromised in the Data Breach, including names, social security numbers, medical and insurance information, lab results and more. The cybercriminals sending these emails demand that patients pay them to prevent the sale of that data."[10]

26. The threatening emails state: "If you are reading this, your data has been stolen and will soon be sold to various data brokers and black markets to be used in fraud and other criminal activities." The threatening emails also include specific examples of the personal data stolen and exposed for the individual recipient of the email, including their name, address, and patient record number, and even contain medical information. As of December 6, 2023, at least 300 patients have contacted Fred Hutch after receiving one of these threatening emails.

27. Following the Data Breach and commencement of its investigation, Fred Hutch took our clinical network offline and implemented additional information technology security protocols.[11]

28. On December 6, 2023, Fred Hutch sent a data breach notice to all current and former patients notifying them of the Data Breach and the risk of harm those individuals now face as a result of the Data Breach.[12]

---

[9] *Id.*

[10] *Id.*

[11] *Update on Data Security Incident*, Fred Hutch Cancer Center, https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited Dec. 7, 2023).

[12] Exhibit A.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

C. Fred Hutch's Failure to Protect Its Patient's Private Information

29. Fred Hutch collects and maintains vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations as a healthcare service provider. The data breach occurred as a direct, proximate, and foreseeable result of multiple failings on the part of Fred Hutch.

30. Fred Hutch inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

31. Fred Hutch failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and the Class Members been aware that Fred Hutch did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Fred Hutch.

32. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. They face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

D. Data Breaches Pose Significant Threats

33. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, are an invaluable commodity and a frequent target of hackers.

34. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

50 compromises short of the current record set in 2021.[13] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just eight shy of the record of 715 set in 2021, and still double that of the number of similar such compromises in 2017.[14]

35. Statista, a German entity that collects and markets data relating to data breach incidents and their consequences, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005; it reported 157 compromises in 2005, to a peak of 1,862 in 2021, to 2022's total of 1,802.[15] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[16]

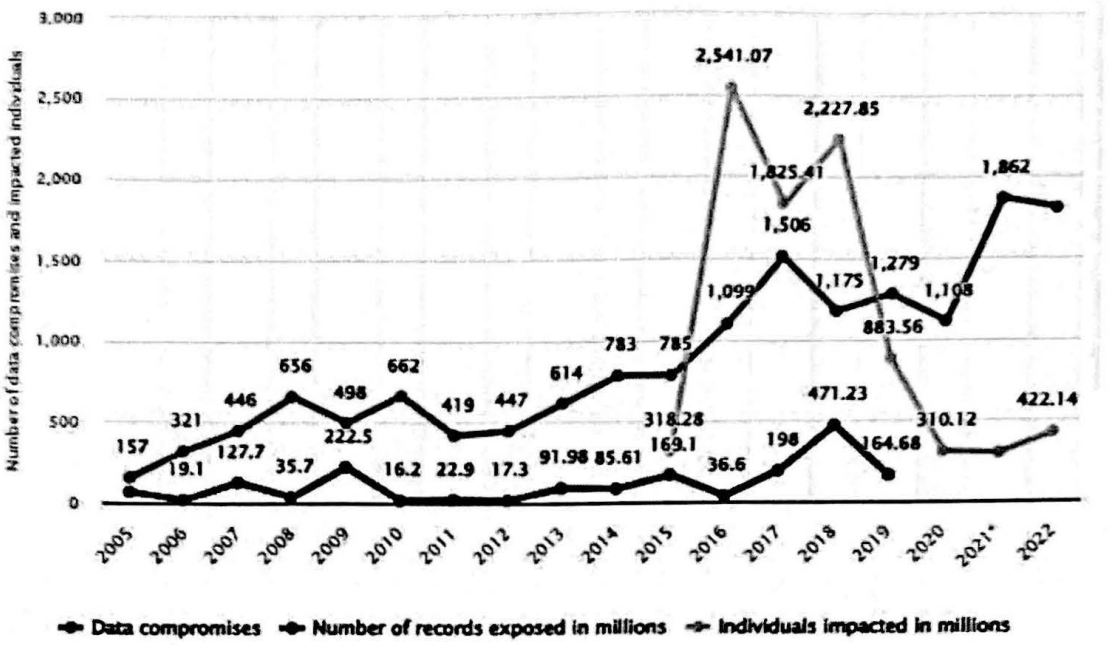
[13] *2022 End of Year Data Breach Report*, Identity Theft Resource Center at 6 (Jan. 25, 2023), *available at* https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report (last accessed Dec. 7, 2023).

[14] *2022 Healthcare Data Breach Report*, The HIPAA Journal (Jan. 24, 2023), *available at* https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed Dec. 7, 2023).

[15] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, *available at* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last accessed Dec. 7, 2023).

[16] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992



36. This stolen Private Information is then routinely traded on dark web black markets as a simple commodity.[17]

37. Armed with just a name and Social Security Number, criminals can fraudulently take out loans under a victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

---

[17] Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (Nov. 15, 2023), *available at* https://cybernews.com/security/whats-your-identity-worth-on-dark-web/ (last accessed Dec. 7, 2023).

[18] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration at 1 (July 2021), available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

The problems associated with a compromised Social Security Number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[19]

38. The most sought after and expensive pieces of information on the dark web are stolen medical records, which command prices from $250 to $1,000 each.[20] Medical records are considered the most valuable because—unlike credit cards, which can easily be canceled, and social security numbers, which can be changed—medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[21] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[22] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical

---

[19] *Id.*

[20] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), available at https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last accessed Dec. 7, 2023).

[21] *Id.*

[22] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), *available at* https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed Dec. 7, 2023); *see also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), *available at* https://www.consumerreports.org/health/medical-identity-theft-a1699327549/ (last accessed Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

treatment.[23] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[24]

39. The wrongful use of compromised medical information is known as medical identity theft, and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[25] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[26]

40. Instances of medical identity theft have grown exponentially over the years, from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[27]

41. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Fred Hutch—which are charged with maintaining and securing patient PII and PHI—should know the importance of protecting that information from unauthorized disclosure. Indeed, Fred Hutch knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint

---

[23] *Id.*
[24] *Id.*
[25] Medical Identity Theft, AARP (March 25, 2022), *available at* https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last accessed Dec. 7, 2023).
[26] *Id.*
[27] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[28]

42. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Fred Hutch on notice of their obligation to safeguard customer and patient information.[29]

43. Given the nature of Fred Hutch's Data Breach, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in their names.

44. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information, because credit card victims can cancel or close credit and debit card accounts.[30] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

---

[28] *See, e.g., Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics (last accessed Dec. 7, 2023).

[29] *See, e.g.*, In the Matter of SKYMED INTERNATIONAL, INC., C-4732, 1923140 (F.T.C. Jan. 26, 2021).

[30] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), *available at* https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Dec. 7, 2023); *see also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), *available at* https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/ (last accessed Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

45. To date, Fred Hutch has not offered its patients identity theft monitoring services.

46. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Fred Hutch failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Fred Hutch's failure to implement or maintain adequate data security measures for its current and former patients.

E. Fred Hutch Had a Duty and Obligation to Protect Private Information

47. Fred Hutch has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and PHI. And third, Fred Hutch imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class members provided, and Fred Hutch obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

48. HIPAA requires, among other things, that Covered Entities and Business Associates implement and maintain policies, procedures, systems, and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI; protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI; regularly review access to data bases containing protected information; and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

49. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . ." 45 CFR § 164.402.

50. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires Fred Hutch to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***." (emphasis added).

51. Upon information and belief, Fred Hutch failed to implement and/or maintain procedures, systems, and safeguards to protect the PII and PHI belonging to Plaintiff and the Class from unauthorized access and disclosure.

52. Upon information and belief, Fred Hutch's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Fred Hutch creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Fred Hutch's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

53. Upon information and belief, Fred Hutch also failed to store the information it collected in a manner that rendered it "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

54. Because Fred Hutch has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class members' injuries, injunctive relief is also necessary to ensure Fred Hutch's approach to information security is adequate and appropriate going forward. Fred Hutch still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiff and Class members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class members' Private Information remains at risk of subsequent data breaches.

2. FTC Act Requirements and Violations

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

56. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[31] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[32] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[33] Fred Hutch clearly failed to do any of the foregoing, as evidenced by the Data Breach itself.

57. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

---

[31] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Dec. 7, 2023).

[32] *Id.*

[33] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

60. As evidenced by the Data Breach, Fred Hutch failed to properly implement basic data security practices. Fred Hutch's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

61. Fred Hutch was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiff and Class members, as Fred Hutch is a sophisticated and technologically savvy healthcare group that relies extensively on technology systems and networks to maintain its practice, including storing its patients' PII, protected health information, and medical information in order to operate its business.

62. Fred Hutch had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information of Plaintiff and the Class from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Fred Hutch and Plaintiff and Class members. Fred Hutch alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

3. Industry Standards and Noncompliance

63. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

64. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Fred Hutch include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Fred Hutch failed to follow some or all of these industry best practices.

65. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Fred Hutch failed to follow these cybersecurity best practices.

66. Fred Hutch should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

67. Upon information and belief, Fred Hutch failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

4. Fred Hutch's Own Stated Policies and Promises

68. Fred Hutch claims that "at Fred Hutchinson Cancer Center, we take the privacy of our patients' health care information seriously."[34]

69. Fred Hutch's own published privacy policy states that: "We are required by law to maintain the privacy and security of your protected health information."[35] The Privacy Policy further promises that Fred Hutch "will not use or share your information other than as described here unless you tell us we can in writing."[36] The only stated exceptions to the requirement for a patient's written consent are for treatment, for payment, for running Fred Hutch's organization, to comply with certain laws, for certain research projects, for organ and tissue donation requests, for work with a funeral director or medical examiner, for certain lawsuits, legal actions, or law enforcement or government requests. The Data Breach met none of those exceptions.

70. Fred Hutch failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information of Plaintiff and Class members.

71. Indeed, Fred Hutch's website states that immediately following the Data Breach it conducted an investigation of the incident, "quarantined the servers," and "implemented additional information technology security protocols." This strongly implies that Fred Hutch's security measures, by their own determination, were inadequate.[37]

---

[34] *Privacy Policy*, Fred Hutch Cancer Center, https://www.fredhutch.org/en/util/patient-policies.html#public-policy (last visited Dec. 7, 2023).

[35] *Joint Notice of Privacy Practices: Your Information. Your Rights. Our Responsibilities.*, Fred Hutch Cancer Center (Dec. 19, 2022), https://www.fredhutch.org/content/dam/www/clinical-pdf/patient-policies/joint-notice-of-privacy-practices.pdf (last visited Dec. 7, 2023).

[36] *Id.*

[37] *Update on Data Security Incident*, Fred Hutch Cancer Center, https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

72. Like any data breach, the Data Breach in this case presents major problems for all affected.[38]

73. The FTC warns the public to pay particular attention to how they keep PII, including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[39]

74. The ramifications of Fred Hutch's failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, medical, or personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

75. PII has a long shelf-life because it can be used in more ways than one, and it typically takes time for an information breach to be detected.

76. Plaintiff and Class members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves, or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI and then risk prosecution by listing it for sale on the dark web if the PII and PHI was not valuable to malicious actors.

---

[38] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), *available at* https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last accessed Dec. 7, 2023).

[39] *Warning Signs of Identity Theft*, Federal Trade Comm'n, *available at* https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

77. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

78. Malicious actors use Private Information to gain access to Class members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

79. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

80. Malicious actors can use Class members' Private Information to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

81. As established above, the PII accessed in the Data Breach is also very valuable to Fred Hutch. Fred Hutch collects, retains, and uses this information to increase profits—it even notes that it will use Class members' data for this reason without their written permission.[40] Fred Hutch patients value the privacy of this information and expect Fred

[40] *See Joint Notice of Privacy Practices: Your Information. Your Rights. Our Responsibilities.*, Fred Hutch Cancer Center (Dec. 19, 2022), https://www.fredhutch.org/content/dam/www/clinical-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

Hutch to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Fred Hutch, provided their PII and PHI, and/or paid the same prices for Fred Hutch's services had they known Fred Hutch did not implement reasonable security measures to protect their PII and PHI. Patients expect that the payments they make to the medical providers incorporate the costs to implement reasonable security measures to protect their Private Information.

82. The Private Information accessed in the Data Breach is also very valuable to Plaintiff and Class members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class members' PII has been compromised and lost significant value.

83. Plaintiffs and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name

pdf/patient-policies/joint-notice-of-privacy-practices.pdf (last visited Dec. 7, 2023). (stating that patient information may be used to "run our practice," "improve care," or used in furtherance of its own "health research").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

until contacted by collections agencies. Plaintiffs and Class members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

84. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

85. Accordingly, Fred Hutch's wrongful actions and inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports," public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[41] The same study also found that identity theft is a deeply traumatic event for victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[42]

86. There is also a high likelihood that significant identity fraud and identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals may be exploited in the future; there is a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

87. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve a data breach in 2023 at $4.45 million.[43] The average cost to

---

[41] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and Protective Factors of Identity Theft Victimization in the United States*, Preventive Medicine Reports, Volume 17 (March 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub (last accessed Dec. 7, 2023).

[42] *Id.*

[43] *Cost of a Data Breach Report 2023*, IBM Security, *available at* https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWa

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[44]

88. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years, and this explosive growth far outstrips the increase in incidence of traditional identity theft.[45] Medical identity theft is especially harmful for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[46]

89. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and health insurance information as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent

---

Oo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds (last accessed Dec. 7, 2023).

[44] *Id.*

[45] Medical Identity Theft, AARP (Mar. 25, 2022), *available at* https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last accessed Dec. 7, 2023).

[46] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

charges, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, monitoring claims made against their health insurance, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; and

e. The loss of Plaintiff's and Class members' privacy.

90. Plaintiff and Class members have suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will continue for years and years. The unauthorized access of Plaintiff's and Class members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely.

91. As a direct and proximate result of Fred Hutch's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

92. In addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose Private Information was accessed in the Data Breach, Plaintiff retains an interest in ensuring there are no future breaches. On information and belief, Fred Hutch is still in possession, custody, or control of Plaintiff's and the Class members' Private Information.

G. Experiences Specific to Plaintiff

Shawna Arneson's Experience

93. Plaintiff Arneson is a current patient of Fred Hutch.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

94. Ms. Arneson received an email from Fred Hutch about the Data Breach. The notice instructed her to "remain vigilant to protect against potential fraud and/or identity theft" implying that her Private Information may have been compromised in the breach.

95. As a result of the Data Breach, Ms. Arneson has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing her financial accounts. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, recreation and rest.

96. As a result of the Data Breach, Plaintiff Arneson has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Arneson is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

97. Plaintiff Arneson suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Fred Hutch obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

98. As a result of the Data Breach, Plaintiff Arenson anticipates spending considerable time and money on an ongoing basis to continue monitoring her accounts and to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

99. Plaintiff brings this action on behalf of herself and, pursuant to CR 23, a Class defined as:

> All persons in the United States whose Private Information was accessed in the Data Breach (the "Class").

Excluded from the Class are Fred Hutch, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

100. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to CR 23, a subclass of:

> All persons who are residents of the State of Washington whose Private Information was accessed in the Data Breach (the "Washington Subclass").

Excluded from the Washington Subclass are Fred Hutch, its executives and officers, and the Judge(s) assigned to this case.

101. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. Reports suggest that the number of affected individuals may be as high as 800,000.[47] The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Fred Hutch and obtainable by Plaintiff only through the discovery process. The members of the Class will be identifiable through information and records in Fred Hutch's possession, custody, and control.

---

[47] *See* Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*, KUOW (Dec. 6, 2023), https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack (last visited Dec. 7, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

102. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Fred Hutch learned of the Data Breach;

b. Whether cybercriminals obtained Class members' Private Information in the Data Breach;

c. Whether Fred Hutch's response to the Data Breach was adequate;

d. Whether Fred Hutch failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Fred Hutch's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Fred Hutch knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Fred Hutch owed a duty to Class members to safeguard their Private Information;

h. Whether Fred Hutch breached its duty to Class members to safeguard their Private Information;

i. Whether Fred Hutch had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;

j. Whether Fred Hutch breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

k. Whether Fred Hutch's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

l. Whether Fred Hutch's conduct was negligent;

m. Whether Fred Hutch was unjustly enriched;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

n. What damages Plaintiff and Class members suffered as a result of Fred Hutch's misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;

p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and

q. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

103. Typicality: All of Plaintiff's claims are typical of the claims of the Class. Upon information and belief, Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Fred Hutch's uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Fred Hutch has acted, and refused to act, on grounds generally applicable to the Class.

104. Adequacy: Plaintiff is an adequate class representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she retained counsel competent and highly experienced in complex class action litigation, and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

105. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Fred Hutch's conduct. It would be virtually impossible for members of the Class individually to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on Fred Hutch's records and databases.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)

106. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

107. Fred Hutch owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Fred Hutch also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

108. Fred Hutch also owes this duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Fred Hutch to use reasonable measures to protect confidential data.

109. Fred Hutch also owes this duty because industry standards mandate that Fred Hutch protect its patients' confidential Private Information.

110. Fred Hutch also owes this duty because it had a special relationship with Plaintiff and Class members. Plaintiff and Class members entrusted their Private Information to Fred Hutch on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Fred Hutch had the ability to protect its systems and the Private Information stored on them from attack.

111. Fred Hutch also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and the Class. This duty exists to allow Plaintiff and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

112. Fred Hutch breached its duties to Plaintiff and the Class by failing to take reasonable appropriate measures to secure, protect, and otherwise safeguard the Private Information belonging to Plaintiff and Class members.

113. Fred Hutch also breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their Private Information had been improperly acquired and accessed.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

114. As a direct and proximate result of Fred Hutch's conduct, Plaintiff and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Permanent increased risk of identity theft.

115. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Fred Hutch, and the damages they suffered were the foreseeable result of Fred Hutch's inadequate security practices.

116. In failing to provide prompt and adequate individual notice of the Data Breach, Fred Hutch also acted with reckless disregard for the rights of Plaintiff and Class Members.

117. Plaintiff is entitled to damages in an amount to be proven at trial and injunctive relief requiring Fred Hutch to, among other things, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)

118. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

119. Plaintiff and the Class provided Fred Hutch with their Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

120. By providing their Private Information, and upon Fred Hutch's acceptance of this information, Plaintiff and the Class, on one hand, and Fred Hutch, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

121. The implied contracts between Fred Hutch and Plaintiff and Class members obligated Fred Hutch to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Fred Hutch expressly adopted and assented to these terms in its public statements, representations and promises as described above.

122. The implied contracts for data security also obligated Fred Hutch to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

123. Fred Hutch breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

124. As a direct and proximate result of Fred Hutch's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

COUNT III
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)

125. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

126. This count is brought in the alternative to Count II.

127. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Fred Hutch.

128. Fred Hutch was benefitted by the conferral upon it of Plaintiff's and Class members' Private Information and by its ability to retain and use that information. Fred Hutch understood that it was in fact so benefitted.

129. Fred Hutch also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential, and its value depended upon Fred Hutch maintaining the privacy and confidentiality of that information.

130. But for Fred Hutch's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Fred Hutch, and Fred Hutch would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiff and Class members, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise, and realizing excessive profits.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

131. As a result of Fred Hutch's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Fred Hutch has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

132. Fred Hutch's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

133. Under the common law doctrine of unjust enrichment, it is inequitable for Fred Hutch to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner.

134. The benefit conferred upon, received, and enjoyed by Fred Hutch was not conferred officiously or gratuitously, and it would be inequitable and unjust for Fred Hutch to retain the benefit.

135. Fred Hutch is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Fred Hutch as a result of its wrongful conduct, including specifically the value to Fred Hutch of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits Fred Hutch receives from the use and sale of that information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

136. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Fred Hutch and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Fred Hutch from its wrongful conduct.

137. Plaintiff and Class Members may not have an adequate remedy at law against Fred Hutch, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code § 19.86.020, *et seq.*
(By Plaintiff on behalf of the Class, or, in the alternative, the Washington Subclass)

138. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

139. Plaintiff and Class members are "persons" under the Washington Consumer Protection Act. RCW 19.86.010(1).

140. Defendant is a "person" as described in the Washington Consumer Protection Act. RCW 19.86.010(1).

141. Fred Hutch is engaged in, and its acts and omissions affect, trade and commerce. Fred Hutch's relevant acts, practices, and omissions complained of in this action were done in the course of Fred Hutch's business of marketing, offering for sale, and selling services throughout Washington and the United States.

142. Fred Hutch is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and many of its employees are residents of the State of Washington.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

143. The Washington Consumer Protection Act prohibits deceptive and unfair acts or practices in the conduct of any business, trade, or commerce, or in the provision of commerce. RCW 19.86.020.

144. In the course of conducting its business, Fred Hutch committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' Private Information. Such practices were likely to cause substantial injury to consumers and were, not reasonably avoidable by consumers and nor outweighed by countervailing benefits.

145. Fred Hutch's conduct was also deceptive. Fred Hutch failed to timely notify and concealed from Plaintiff and Class Members the inadequacy of its data security measures and the unauthorized release and disclosure of their Private Information. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information, medical information, and identities.

146. Fred Hutch's unfair and deceptive acts or practices in the conduct of business include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

147. Fred Hutch's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

148. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should or could have reasonably avoided.

149. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct and proximate result of Fred Hutch's unfair and deceptive acts and practices as set forth herein include, without limitation:

a. theft of their Private Information;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and health insurance;

c. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. damages to and diminution in value of their Private Information entrusted to Fred Hutch, and with the understanding that it would safeguard their data against theft and not allow access and misuse of their data by others; and

f. the continued risk to their Private Information, which remains in the possession of Fred Hutch and which is subject to further breaches so long as it fails to undertake appropriate and adequate measures to protect data in its possession.

150. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Fred Hutch from disclosing their Private Information without their consent and prohibiting Fred Hutch from continuing its wrongful conduct; reasonable attorneys' fees and costs; treble damages for each Class member, not to exceed $25,000 per Class member; and any other relief that is just and proper under RCW 19.86.090.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Fred Hutch, as follows:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL 206.682.5600 • FAX 206.682.2992

A. That the Court certify this action as a class action, proper and maintainable pursuant to CR 23; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Fred Hutch from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, and treble damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution;

I. That the Court grant leave to amend these pleadings to conform to evidence produced at trial; and

J. That the Court grant all other relief as it deems just and proper.

Date: December 7, 2023

Respectfully Submitted,

s/ Kim D. Stephens, P.S.

Kim D. Stephens, P.S., WSBA #11984
Cecily C. Jordan, WSBA #50061
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992
kstephens@tousley.com
cjordan@tousley.com

Attorneys for Plaintiff and the Proposed Class